Discrete Applied Mathematics 157 (2009) 2892–2903

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Cyclic and negacyclic codes over the Galois ring GR(p^2, m)

R. Sobhani, M. Esmaeili *

Department of Mathematical Sciences, Isfahan University of Technology, 84156-83111, Isfahan, Iran

ARTICLE INFO

Article history:
Received 7 November 2006
Received in revised form 27 February 2009
Accepted 2 March 2009
Available online 26 March 2009

Keywords:
Cyclic codes
Galois rings

ABSTRACT

This paper deals with cyclic codes over the Galois ring GR(p^2, m). A unique set of generators for these codes and an algorithm for finding these generators are presented. The form of dual codes is studied. The obtained results on cyclic codes are extended to the class of negacyclic codes.

1. Introduction

The discovery of good nonlinear codes from linear codes over $\mathbb{Z}_4$, via the Gray map motivated the study of cyclic codes over rings in general [13]. It has been shown in [13] that the polynomial X^3+X+1 generating the binary Hamming code of length 7 over $\mathbb{F}_2$, lifts to the polynomial X^3+2X^2+X+3 that generates a cyclic code over the ring $\mathbb{Z}_4$. Extending this code over $\mathbb{Z}_4$, by adding an overall parity-check symbol, produces the octacode whose Gray image is equivalent to the well-known nonlinear Nordstrom–Robinson code [13].

Cyclic codes over rings form an important class of linear codes due to their rich algebraic structure. Given a ring R, these codes are in correspondence with ideals in the polynomial ring $R[X]/\langle X^N-1\rangle$, where N is the length of the code. In the case $R=\mathbb{Z}_{p^e}$ and $(N,p)=1$, these codes are well-understood objects [7,14]. But when p divides N the characterization of the corresponding codes is not that easy. Substantial research work concerning these codes has been developed in [2,4,11,12,16]. Cyclic codes over $\mathbb{Z}_4$ of length $2n$ with n odd, were studied in [4], and the codes of length 2^n were examined in [2], while codes of arbitrary even length were studied in [11]. Generalizing the method used in [4] and [11], cyclic codes of arbitrary length N over the ring $\mathbb{Z}_{p^e}$ were studied in [12]. The authors applied a discrete Fourier transform approach to define an isomorphism between the polynomial ring $\mathbb{Z}_{p^e}[X]/\langle X^N-1\rangle$ and a direct sum of certain local rings. They have considered a general form of generators for ideals of component rings, [12, Theorm 6.5]. Using these generators and analyzing the inverse image of the mentioned isomorphism, they tried to obtain a polynomial representation for ideals of the ring $\mathbb{Z}_{p^e}[X]/\langle X^N-1\rangle$. They even considered cyclic codes of arbitrary length over the ring $\mathbb{Z}_{p^e}$, but with a cumbersome method leading to a complicated generators.

Another form of generators for cyclic codes over a finite chain ring can be found in [6,15,16,18]. These generators are based on the concept of Gröbner basis and seems to be simpler. Since the Galois rings GR(p^e, m) are chain rings, these generators can be used to describe cyclic codes over GR(p^e, m). However an important step in classifying these codes is to find the mentioned generators explicitly. Unfortunately finding all of these generators for cyclic codes over GR(p^e, m) is a tedious process. The main goal of this paper is to find these generators for cyclic and negacyclic codes over GR(p^2, m).

We should mention that though our approach is different from the one employed in [11], in some cases our results coincide with those given in [11] (see also [2,1]). This happens precisely when $e=2$ and $N=p^n$. Results of this type are given in Section 4. These results can be proved by modifying the corresponding results in [11] to work for arbitrary prime p.

* Corresponding author. Tel.: +98 311 391 3631; fax: +98 311 391 2602.
E-mail addresses: sbnreza@math.iut.ac.ir (R. Sobhani), emorteza@cc.iut.ac.ir (M. Esmaeili).

0166-218X/$ – see front matter
doi:10.1016/j.dam.2009.03.001

Let us have some notation and definitions. Let R be a finite commutative ring with identity. A code C of length N over R is a subset of R^N. If C is a submodule of R^N then C is said to be linear. In this work we assume that C is linear unless otherwise stated. Suppose that $\mathbf{u} = (u_0, u_1, \ldots, u_{N-1})$ and $\mathbf{v} = (v_0, v_1, \ldots, v_{N-1})$ are in C. The standard inner product of $\mathbf{u}$ and $\mathbf{v}$, denoted $\mathbf{u}.\mathbf{v}$, is $\mathbf{u}.\mathbf{v} = u_0v_0 + u_1v_1 + \cdots + u_{N-1}v_{N-1}$. The dual code of C is defined by $C^\perp := \{\mathbf{w} | \mathbf{w}.\mathbf{v} = 0 \text{ for all } \mathbf{v} \in C\}$. We say C is self-dual if $C = C^\perp$. Let $R = \mathrm{GR}(p^2, m)$. For C, a linear code of length N over R, we consider the following two linear codes over $\mathbb{F}_{p^m}$. The first is the code $\{\mathbf{c} \bmod p \mid \mathbf{c} \in C\}$ which is called *the residue code* of C and is denoted by $\mathrm{Res}(C)$, and the second one is the code $\{\mathbf{c} \in \mathbb{F}_{p^m}^N \mid p\,\mathbf{c} \in C\}$ which is called *the torsion code* of C and is denoted by $\mathrm{Tor}(C)$. Theorem 3.5 of [17] indicates that $|C| = |\mathrm{Res}(C)||\mathrm{Tor}(C)|$. A code C of length N over R is said to be cyclic if $(c_0, c_1, \ldots, c_{N-1}) \in C$ implies $(c_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in C$. We use the natural correspondence between cyclic codes over R and ideals of the ring $R[X]/\langle X^N - 1\rangle$, where $\mathbf{c} = (c_0, c_1, \ldots, c_{N-1})$ is viewed as $c_0 + c_1X + \cdots + c_{N-1}X^{N-1}$. For a unit $a \in R$ and a code C over R, if $(c_0, c_1, \ldots, c_{N-1}) \in C$ implies $(ac_{N-1}, c_0, c_1, \ldots, c_{N-2}) \in C$ then the code is said to be constacyclic. Trivially constacyclic codes are a natural generalization of cyclic codes by letting $a = 1$. Similar to cyclic codes, there is a natural correspondence between constacyclic codes and ideals of the ring $R[X]/\langle X^N - a\rangle$. In the case $a = -1$, this class of codes are known as negacyclic codes.

Negacyclic codes of odd length over $\mathbb{Z}_4$ were studied in [19] and those of even length (by using a discrete Fourier transform approach) were studied in [5]. In general, results of [10] classify negacyclic codes of length prime to p over the Galois ring $\mathrm{GR}(p^e, m)$ for arbitrary prime p and positive integer e. Also negacyclic codes of length a power of 2 over the Galois ring $\mathrm{GR}(2^e, m)$ were studied in [9]. We shall extend our results on cyclic codes to the class of negacyclic codes (see Section 5).

The structure of the paper is as follows. Section 2 is devoted to an explicit classification of ideals of the ring $\mathrm{GR}(p^2, m)[X]/\langle X^N - 1\rangle$. Duals of these ideals are discussed in Section 3. In Section 4 we deal with the case where $N = p^n$ and describe the form of self-dual ideals in this case. More precisely, a part of the results presented in [11] for $p = 2$ is generalized to arbitrary prime p (see also [2,1]). In Section 5 we extend our results to the class of negacyclic codes.

2. Distinct ideals of $\mathrm{GR}(p^2, m)/\langle X^N - 1\rangle$

Let us denote by $\mathscr{R}$ the ring $\mathrm{GR}(p^2, m)/\langle X^N - 1\rangle$. In this paper, by an ideal of the ring $\mathscr{R}$ we mean a cyclic code of length N over $\mathrm{GR}(p^2, m)$. In this section we determine all distinct ideals of $\mathscr{R}$. For $\mathscr{I}$, an ideal of $\mathscr{R}$, it can be easily seen that $\mathrm{Tor}(\mathscr{I})$ and $\mathrm{Res}(\mathscr{I})$ are ideals of $\mathbb{F}_{p^m}[X]/\langle X^N - 1\rangle$ and $\mathrm{Tor}(\mathscr{I}) \subseteq \mathrm{Res}(\mathscr{I})$. Hence we have $\mathrm{Res}(\mathscr{I}) = \langle f(X)\rangle$ and $\mathrm{Tor}(\mathscr{I}) = \langle h(X)\rangle$, where $h(X) \mid f(X) \mid X^N - 1$ in $\mathbb{F}_{p^m}[X]$. Let τ_m be the well-known Teichmüller set of coset representatives of $\mathrm{GR}(p^2, m)$ modulo $\langle p\rangle$. Recall that any polynomial $A(X)$ in $\mathscr{R}$ can be represented as $A_0(X) + pA_1(X)$, where $A_i(X) \in \tau_m[X]$ for $i \in \{0, 1\}$. In what follows we assume that $N = p^nk$, where $(p, k) = 1$, and $X^N - 1 = f_1(X)^{p^n}f_2(X)^{p^n} \ldots f_r(X)^{p^n}$ is the unique factorization of the polynomial $X^N - 1$ over the field $\mathbb{F}_{p^m}$. Moreover, we do not make distinction between the field $\mathbb{F}_{p^m}$ and the set τ_m.

Theorem 2.1. *Let $\mathscr{I}$ be an ideal of $\mathscr{R}$ with $\mathrm{Res}(\mathscr{I}) = \langle f(X)\rangle$ and $\mathrm{Tor}(\mathscr{I}) = \langle h(X)\rangle$, where $h(X) \mid f(X) \mid X^N - 1$ over $\mathbb{F}_{p^m}$. Assume that $f(X) = f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r}$, where $0 \le j_i \le p^n$. Then $\mathscr{I} = \langle f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r} + pg(X), ph(X)\rangle$, where the polynomial $f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r}$ is calculated in $\mathscr{R}$ and $g(X) = 0$ or $\deg(g(X)) < \deg(h(X))$. Moreover, these generators of $\mathscr{I}$ are unique.*

Proof. According to Theorem 4.2 of [16], $\mathscr{I}$ admits a set of generators of the form $\{A(X), pB(X)\}$ such that $B(X) \mid \overline{A(X)} \mid X^N - 1$ over $\mathbb{F}_{p^m}$ and we have $\deg(B(X)) < \deg(A(X))$, where $\overline{A(X)}$ stands for $A(X) \bmod p$. It is easily seen that $B(X) = h(X)$ and $\overline{A(X)} = f(X)$. Let

$$A(X) := f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r} + pg_1(X),$$

where $f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r}$ is calculated in $\mathscr{R}$. Divide the polynomial $g_1(X)$ by $h(X)$. Assume that $g_1(X) = h(X)q(X) + g(X)$ where $\deg(g(X)) < \deg(h(X))$. A straightforward verification shows that $f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r} + pg(X)$ lies in $\mathscr{I}$ and we have $\mathscr{I} = \langle f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r} + pg(X), ph(X)\rangle$. Next we check the uniqueness. Clearly the generator $ph(X)$ is unique. If $\mathscr{I}$ contains another polynomial of the form $f_1(X)^{j_1}f_2(X)^{j_2} \ldots f_r(X)^{j_r} + pl(X)$ for some polynomial $l(X)$ with $\deg(l(X)) < \deg(h(X))$ then we must have $p(g(X) - l(X)) \in \mathscr{I}$ and hence $g(X) - l(X) \in \mathrm{Tor}(\mathscr{I})$. Since $\mathrm{Tor}(\mathscr{I}) = \langle h(X)\rangle$ and $\deg(g(X) - l(X)) < \deg(h(X))$, we must have $l(X) = g(X)$. The proof is now completed. ■

Now we determine ideals of $\mathscr{R}$ in the form presented above. If $\mathrm{Res}(\mathscr{I}) = 0$ or equivalently $f(X) = X^N - 1$ then we have $\mathscr{I} = \langle ph(X)\rangle$. Ideals of this type can be easily found. To determine ideals of $\mathscr{R}$ with nonzero residue ideal, we need the following Lemma. Recall that $N = p^nk$, where $(k, p) = 1$. If $n = 0$ then ideals of $\mathscr{R}$ are well characterized in [7]. Hence, we assume that $n \ge 1$.

Lemma 2.2. *In $\mathscr{R}$ we have $(X^k - 1)^{p^n} = p(X^k - 1)^{p^{n-1}}\mathscr{K}(X)$, where*

$$\mathscr{K}(X) = \sum_{j=0}^{p-2} \frac{(-1)^{j+1}}{j+1}(X^k - 1)^{jp^{n-1}} \in \mathbb{F}_{p^m}[X].$$

In particular, $\mathscr{K}(X)$ is a unit in $\mathscr{R}$.

Proof. See the Appendix. □

For $f(X) = f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r}$, a divisor of $X^N - 1$, we denote by $\widehat{f(X)}$ the polynomial $(X^N - 1)/f(X)$, i.e. $\widehat{f(X)} = f_1(X)^{p^n - j_1} f_2(X)^{p^n - j_2} \dots f_r(X)^{p^n - j_r}$.

Theorem 2.3. *Let $\mathcal{I} = \langle f(X) + pg(X) \rangle$ be a principal ideal of the ring $\mathcal{R}$, where $f(X) = f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r}$ is a proper divisor of $X^N - 1$ and $\deg(g(X)) < \deg(f(X))$ or $g(X) = 0$. Set $A(X) := (X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)} \in \mathbb{F}_{p^m}[X]$. Then we have* $\mathrm{Tor}(\mathcal{I}) = \langle \gcd(f(X), A(X)) \rangle$.

Proof. Let $\mathrm{Tor}(\mathcal{I}) = \langle h(X) \rangle$. Since $pf(X) \in \mathcal{I}$, the polynomial $h(X)$ must divide $f(X)$. Furthermore, using Lemma 2.2, we have

$$\begin{aligned} \widehat{f(X)}(f(X) + pg(X)) &= [f_1(X) f_2(X) \dots f_r(X)]^{p^n} + pg(X)\widehat{f(X)} \\ &= (X^k - 1)^{p^n} + pg(X)\widehat{f(X)} \\ &= p(X^k - 1)^{p^n - 1}\mathcal{K}(X) + pg(X)\widehat{f(X)} \\ &= pA(X). \end{aligned}$$

Hence $h(X)$ must divide $A(X)$. On the other hand, since $\mathrm{Tor}(\mathcal{I}) = \langle h(X) \rangle$, there exists a polynomial $a(X) + pb(X)$ such that $(f(X) + pg(X))(a(X) + pb(X)) = ph(X)$. This equality shows that $p \mid f(X)a(X)$ and hence $\widehat{f(X)} \mid a(X)$. Write $a(X) = \widehat{f(X)}c(X)$. Using Lemma 2.2, one can deduce that $h(X) = c(X)A(X) + b(X)f(X)$. Now the assertion follows. ■

The following theorem enables us to determine the unique form of those ideals of $\mathcal{R}$ which have nonzero residue ideal.

Theorem 2.4. *Let $\mathcal{I} = \langle f(X) + pg(X), ph(X) \rangle$ be an ideal of the ring $\mathcal{R}$, where $f(X) = f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r}$ is a proper divisor of $X^N - 1$, $h(X) \mid f(X) \mid X^N - 1$ in $\mathbb{F}_{p^m}[X]$ and $\deg(g(X)) < \deg(h(X))$ or $g(X) = 0$. Then $\mathcal{I}$ is in the unique form if and only if $h(X) \mid (X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)}$ in $\mathbb{F}_{p^m}[X]$.*

Proof. Set $A(X) := (X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)}$ and assume that $\mathcal{I}$ is in the unique form. Consequently, by Theorem 2.1, we must have $\mathrm{Tor}(\mathcal{I}) = \langle h(X) \rangle$. On the other hand, by Theorem 2.3 we have

$$\mathrm{Tor}(\langle f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r} + pg(X) \rangle) = \langle \gcd(f(X), A(X)) \rangle .$$

Since $\langle f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r} + pg(X) \rangle \subseteq \mathcal{I}$ we must have $h(X) \mid A(X)$, as desired. Conversely, assume that $h(X) \mid A(X)$. To show that $\mathcal{I}$ is in the unique form, by Theorem 2.1 we need to prove $\mathrm{Tor}(\mathcal{I}) = \langle h(X) \rangle$. Assume that $a_1(X) + pa_2(X)$, $b_1(X) + pb_2(X)$ and $l(X)$ satisfy

$$(a_1(X) + pa_2(X))(f(X) + pg(X)) + (b_1(X) + pb_2(X))(ph(X)) = pl(X).$$

Applying an argument similar to the one used in the proof of Theorem 2.3, one can show that $\gcd(A(X), f(X), h(X)) \mid l(X)$. Since $h(X) \mid \gcd(A(X), f(X))$ we can conclude that $h(X) \mid l(X)$. This shows $\mathrm{Tor}(\mathcal{I}) = \langle h(X) \rangle$ and the proof is complete. ■

Corollary 2.5. *Suppose that $\mathcal{I} = \langle f(X) + pg(X),\ ph(X) \rangle$ is an ideal of the ring $\mathcal{R}$, where $f(X) = f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r}$ is a proper divisor of $X^N - 1$, $\deg(g(X)) < \deg(h(X))$ or $g(X) = 0$, and $h(X) \mid \gcd(f(X), X^{N/p} - 1, \widehat{f(X)})$. Then $\mathcal{I}$ is in the unique form.* □

We now summarize our results in the following algorithm, which determines the unique form of all distinct ideals of the ring $\mathcal{R}$.

Algorithm: For all $f(X) = f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r}$, a divisor of $X^N - 1$ in $\mathbb{F}_{p^m}[X]$, and for all $h(X)$ a divisor of $f(X)$ do:

(1) If $f(X) = X^N - 1$ then $\mathcal{I} = \langle ph(X) \rangle$ is in the unique form.
(2) If $f(X) \neq X^N - 1$ then,
   (a) If $h(X) \mid \gcd(X^{N/p} - 1, \widehat{f(X)})$, then for any $g(X)$ with $\deg(g(X)) < \deg(h(X))$ or $g(X) = 0$, the ideal $\mathcal{I} = \langle f(X) + pg(X), ph(X) \rangle$ is in the unique form.
   (b) If $h(X) \nmid \gcd(X^{N/p} - 1, \widehat{f(X)})$, then we may find those polynomials $g(X)$ with $\deg(g(X)) < \deg(h(X))$ or $g(X) = 0$, such that in $\mathbb{F}_{p^m}[X]$:
   $$h(X) \mid (X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)}.$$

Remark 2.6. In the subcase (b) above, our aim is to find polynomials $g(X)$ with $\deg(g(X)) < \deg(h(X))$ or $g(X) = 0$, such that in $\mathbb{F}_{p^m}[X]$ we have $h(X) \mid (X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)}$. Let $C = \langle h(X) \rangle$ be the repeated-root cyclic code of length N over $\mathbb{F}_{p^m}$ generated by $h(X)$. Hence we are interested in polynomials $g(X) \in \mathbb{F}_{p^m}[X]$ with $\deg(g(X)) < \deg(h(X))$ or $g(X) = 0$, such that $(X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)}$ lies in C. Let $\mathbf{v}$ be the vector representation of $(X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)}$ and H be a parity-check matrix for C. Note that parity-check matrices of repeated-root cyclic codes over $\mathbb{F}_{p^m}$ have been introduced in [8]. Now one can solve the equation $\mathbf{v}H^t = 0$ in order to find all the polynomials $g(X)$ with the desired property. Note that for small values of N, p and m, one can directly calculate polynomial $g(X)$ from the relation $h(X) \mid (X^{N/p} - 1)\mathcal{K}(X) + g(X)\widehat{f(X)}$. □

Example 2.7. In this example, using the algorithm presented above, we give the unique form of all distinct ideals of the ring $\mathbb{Z}_4[X]/\langle X^6-1\rangle$. Note that when an ideal $\mathcal{I}=\langle f(X)+2g(X), 2h(X)\rangle$ can be principally generated by $f(X)+pg(X)$ then the second generator $2h(X)$ is removed from its representation.

$$\langle 0\rangle, \langle 2\rangle, \langle 2(X+1)\rangle, \langle 2(X^2+1)\rangle, \langle 2(X^2+X+1)\rangle, \langle 2(X^2+X+1)^2\rangle, \langle 2(X^3+1)\rangle,$$
$$\langle 2(X^3+1)(X^2+X+1)\rangle, \langle 2(X^3+1)(X+1)\rangle,$$
$$\langle 1\rangle, \langle (X+1)\rangle, \langle (X+1)+2\rangle, \langle (X^2+X+1)\rangle, \langle (X^2+X+1)+2\rangle, \langle (X^2+X+1)+2X\rangle,$$
$$\langle (X^2+X+1)+2(X+1)\rangle, \langle (X+1)^2\rangle, \langle (X+1)^2+2(X+1)\rangle, \langle (X^2+X+1)^2\rangle,$$
$$\langle (X^2+X+1)^2+2X(X^2+X+1)\rangle, \langle (X+1)(X^2+X+1)\rangle, \langle (X+1)(X^2+X+1)+2\rangle,$$
$$\langle (X+1)(X^2+X+1)+2X\rangle, \langle (X+1)(X^2+X+1)+2(X+1)\rangle, \langle (X+1)(X^2+X+1)+2X^2\rangle,$$
$$\langle (X+1)(X^2+X+1)+2(X^2+1)\rangle, \langle (X+1)(X^2+X+1)+2(X^2+X)\rangle,$$
$$\langle (X+1)(X^2+X+1)+2(X^2+X+1)\rangle, \langle (X+1)^2(X^2+X+1)\rangle, \langle (X+1)^2(X^2+X+1)+2\rangle,$$
$$\langle (X+1)^2(X^2+X+1)+2X\rangle, \langle (X+1)^2(X^2+X+1)+2(X+1)\rangle,$$
$$\langle (X+1)^2(X^2+X+1)+2(X^2+1)\rangle, \langle (X+1)^2(X^2+X+1)+2X(X+1)\rangle,$$
$$\langle (X+1)^2(X^2+X+1)+2(X^3+1)\rangle, \langle (X+1)^2(X^2+X+1)+2X^2(X+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)^2\rangle, \langle (X+1)(X^2+X+1)^2+2\rangle,$$
$$\langle (X+1)(X^2+X+1)^2+2(X^2+X+1)\rangle, \langle (X+1)(X^2+X+1)^2+2X(X^3+1)\rangle,$$
$$\langle (X+1), 2\rangle, \langle (X^2+X+1), 2\rangle, \langle (X+1)^2, 2\rangle, \langle (X^2+X+1)^2, 2\rangle, \langle (X+1)(X^2+X+1), 2\rangle,$$
$$\langle (X+1)(X^2+X+1), 2(X+1)\rangle, \langle (X+1)(X^2+X+1), 2(X^2+X+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)+2, 2(X+1)\rangle, \langle (X+1)(X^2+X+1)+2, 2(X^2+X+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)+2X, 2(X^2+X+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)+2(X+1), 2(X^2+X+1)\rangle,$$
$$\langle (X+1)^2(X^2+X+1), 2\rangle, \langle (X+1)^2(X^2+X+1), 2(X+1)\rangle,$$
$$\langle (X+1)^2(X^2+X+1), 2(X^2+X+1)\rangle, \langle (X+1)^2(X^2+X+1)+2(X+1), 2(X^2+1)\rangle,$$
$$\langle (X+1)^2(X^2+X+1)+2(X+1), 2(X^2+X+1)\rangle,$$
$$\langle (X+1)^2(X^2+X+1)+2(X+1), 2(X^3+1)\rangle,$$
$$\langle (X+1)^2(X^2+X+1)+2X(X+1), 2(X^3+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)^2, 2\rangle, \langle (X+1)(X^2+X+1)^2, 2(X+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)^2, 2(X^2+X+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)^2+2(X^2+X+1), 2(X^2+X+1)\rangle,$$
$$\langle (X+1)(X^2+X+1)^2+2(X^2+X+1), 2(X^3+1)\rangle.$$

Remark 2.8. Recall that Theorem 3.4 of [18], indicates that the ring $\mathcal{R}$ has non-principal ideals. It is now a warning that if $\mathcal{I}=\langle f(X)+pg(X), ph(X)\rangle$ is an ideal of the ring $\mathcal{R}$ in the unique form, then $\mathcal{I}$ does not need to be a non-principal ideal even if $ph(X)\notin\langle f(X)+pg(X)\rangle$. To see this note that in the above example we have

$$\langle (X+1)(X^2+X+1)^2+2(X^2+X+1), 2(X^3+1)\rangle=\langle (X+1)(X^2+X+1)^2+2X(X^2+X+1)\rangle.$$

However, as we shall see in Remark 4.2, in the case $N=p^n$, such ideals are non-principal. □

3. Dual codes

Let $\mathcal{I}$ be an ideal of the ring $\mathcal{R}$ and C be its corresponding cyclic code. Since the dual of C is also cyclic, we can discuss about the ideal corresponding to the cyclic code $C^{\perp}$. Let us denote this by $\mathcal{I}^{\perp}$. In this part we describe the unique form of the ideal $\mathcal{I}^{\perp}$. We start with the following two definitions.

Definition 3.1. Let $\mathcal{I}$ be an ideal of $\mathcal{R}$. The *annihilator* of $\mathcal{I}$ is defined to be the ideal $A(\mathcal{I}):=\{g(X)\mid g(X)f(X)=0 \text{ for all } f(X)\in\mathcal{I}\}$.

Definition 3.2. Let $f(X)=\sum_{i=0}^{N-1}a_iX^i$ be an element of $\mathcal{R}$. The reciprocal of $f(X)$, denoted $f^*(X)$, is the element $\sum_{i=0}^{N-1}a_iX^{N-i}$ of $\mathcal{R}$. For any subset E of $\mathcal{R}$, the set $\{e^*\mid e\in E\}$ is denoted by E^*.

The following Lemma is the same as Corollary 18 of [2] with the exception that we have replaced the ring $\mathbb{Z}_4$ with the ring $\mathrm{GR}(p^2, m)$.

Lemma 3.3. *Let $\mathcal{I}$ be an ideal of the ring $\mathcal{R}$. Then $\mathcal{I}^{\perp}=A(\mathcal{I})^*$.* □

Theorem 3.4. *Let $\mathcal{I} = \langle f(X) + pg(X), ph(X)\rangle$ be an ideal of $\mathcal{R}$ in the unique form. Then there exists a unique polynomial $l(X) \in \mathcal{R}$ such that $l(X) = 0$ or $\deg(l(X)) < \deg(\widehat{f(X)})$ and $(f(X) + pg(X))(\widehat{h(X)} + pl(X)) = 0$. Moreover, setting $a := \deg(\widehat{h(X)}) - \deg(l(X))$ we have $\mathcal{I}^{\perp} = \langle F(X) + pG(X), pH(X)\rangle$, where $F(X) = \widehat{h(X)}^*$, $H(X) = \widehat{f(X)}^*$ and $G(X) = X^a l^*(X)$ mod $H(X)$.*

Proof. Let $\langle f_1(X) + pg_1(X), ph_1(X)\rangle$ be the unique form of the ideal $A(\mathcal{I})$. Since $ph_1(X)(f(X) + pg(X)) = 0$, the polynomial $f(X)h_1(X)$ is divisible by p and hence $\widehat{f(X)} \mid h_1(X)$. On the other hand, $p\widehat{f(X)}(f(X)+pg(X)) = 0$ implying that $h_1(X) = \widehat{f(X)}$. Similarly, one can see that $f_1(X) = \widehat{h(X)}$. Setting $l(X) := g_1(X)$, we have proved the first claim of the Theorem. The second assertion follows from Lemmas 19 and 20 of [2]. ■

Example 3.5. Using Theorem 3.4 and Example 2.7, we show that there are three cyclic self-dual codes of length 6 over the ring $\mathbb{Z}_4$, namely

$$\mathcal{I}_1 = \langle 2\rangle, \qquad \mathcal{I}_2 = \left\langle (X^3+1)(X+1)+2\right\rangle, \qquad \mathcal{I}_3 = \left\langle (X^3+1)(X+1)+2X\right\rangle.$$

We mention that $\mathrm{Tor}(\mathcal{I}_2) = \mathrm{Tor}(\mathcal{I}_3) = \left\langle X^2+X+1\right\rangle$. Clearly $\mathcal{I}_1$ is self-dual. Using Theorem 3.4, it is easy to verify that $A(\mathcal{I}_2) = \mathcal{I}_3$. On the other hand, we have

$$\mathcal{I}_3^* = \left\langle (X^3+1)(X+1)+2X^3, 2(X^2+X+1)\right\rangle = \left\langle (X^3+1)(X+1)+2\right\rangle = \mathcal{I}_2.$$

Hence $\mathcal{I}_2$ is self-dual. For the ideal $\mathcal{I}_3$, we note that $A(\mathcal{I}_3) = A(A(\mathcal{I}_2)) = \mathcal{I}_2$ and $\mathcal{I}_2^* = (\mathcal{I}_3^*)^* = \mathcal{I}_3$. Hence $\mathcal{I}_3$ is also self-dual. Finally, it follows from Theorem 3.4 that the remaining ideals listed in Example 2.7 cannot be self-dual.

Remark 3.6. Rather than the argument applied to the above example, one can check by hand or using a computer that the three codes presented above are self-dual. This shows that Corollary 2 in [4] has problem since it indicates that there exists only one cyclic self-dual code of length 6 over $\mathbb{Z}_4$, namely the code $\langle 2\rangle$. Nevertheless, we investigate the problem of the mentioned corollary in more detail. With notation as in [4], it has been indicated in the proof of the corollary that $C_i = C_{n-i}$ for all i. However, from the hypothesis of the corollary one can just deduce that i and $n-i$ are in the same cyclotomic coset and hence C_{n-i} is equal with $C_i^{f^a}$, where f is the Frobenious map, a is such that $-1 \cong 2^a \bmod n$ and f^a denotes the a-times combination of the map f with itself. On the other hand, in general one cannot deduce that $C_i = C_i^{f^a}$. To see this, assume that $n = 3$ and $\tau_2 = \{0, 1, \zeta, \zeta^2\}$. Note that we are using notation of [4]. Now consider the code $C = C_0 \oplus C_1 = \langle 2\rangle \oplus \langle u - 1 + 2\zeta\rangle$. Here we have $C_2 = C_1^f = \left\langle u - 1 + 2\zeta^2\right\rangle$ and hence $C_2 \neq C_1$. □

4. The case $N = p^n$

In this section we assume that $N = p^n$, equivalently $k = 1$, and generalize a part of the results given in [11] for $p = 2$, to arbitrary prime p (see also [2] and [1]). These results can also be proved by modifying the corresponding results in [11] to work for p. As a consequence of Theorem 2.3, we state the following theorem, which is a generalization of Proposition 2.5 of [11] to an arbitrary prime p (see also Theorems 11 and 12 of [2]).

Theorem 4.1. *Let $\mathcal{I} = \left\langle (X-1)^s + p(X-1)^t h(X)\right\rangle$ be an ideal of $\mathcal{R}$, where $h(X) = \sum_{i=0}^{s-t-1} a_i(X-1)^i$ is either a unit or the zero polynomial. Suppose $\mathrm{Tor}(\mathcal{I}) = \left\langle (X-1)^T\right\rangle$. Then we have the following possibilities:*

(A) $h(X) \neq 0$.
  (1) *If $p^n + t - s \neq p^{n-1}$, then $T = \min\{s, p^{n-1}, p^n + t - s\}$.*
  (2) *If $p^{n-1} = p^n + t - s$ and $a_0 \neq 1$, then $T = p^{n-1}$.*
  (3) *If $p^{n-1} = p^n + t - s$ and $a_0 = 1$, then*
    (a) *If $h(X) + \mathcal{K}(X) = 0 \pmod p$, then $T = s$.*
    (b) *If $h(X) + \mathcal{K}(X) = (X-1)^v \widetilde{h}(X)$ for some unit $\widetilde{h}(X)$, then*
      $T = \min\{s, p^{n-1} + v\}$

(B) $h(X) = 0$. *In this case we have $T = \min\{s, p^{n-1}\}$.* □

Remark 4.2. Recall that according to Theorem 3.4 of [18] (see also Lemma 3 in [3]), $\mathcal{R}$ contains non-principal ideals. Here we characterize principal and non-principal ideals of $\mathcal{R}$. According to Theorem 2.1, any ideal $\mathcal{I}$ of $\mathcal{R}$ with $\mathrm{Res}(\mathcal{I}) = \langle (X-1)^s\rangle$ and $\mathrm{Tor}(\mathcal{I}) = \left\langle (X-1)^T\right\rangle$ is of the form

$$\mathcal{I} = \left\langle (X-1)^s + p(X-1)^t \sum_{i=0}^{T-t-1} a_i(X-1)^i, p(X-1)^T\right\rangle,$$

where $\sum_{i=0}^{s-t-1} a_i(X-1)^i$ is either a unit or the zero polynomial. Now set

$$\mathcal{J} := \left\langle (X-1)^s + p(X-1)^t \sum_{i=0}^{T-t-1} a_i(X-1)^i \right\rangle \subseteq \mathcal{I}.$$

We have the following two possibilities:

(1) $p(X-1)^T \in \mathcal{J}$. In this case $\mathcal{I} = \mathcal{J}$ is principal and can be obtained using Theorem 4.1.
(2) $p(X-1)^T \notin \mathcal{J}$. Consequently, $\mathrm{Tor}(\mathcal{J}) = \langle (X-1)^L \rangle$ for some $L > T$, and hence $\mathcal{I}$ is obtained from the principal ideal $\mathcal{J}$ by adding the term $p(X-1)^T$ to $\mathcal{J}$. Note that ideals of this type cannot be principally generated. To see this assume $\mathcal{I} = \left\langle (X-1)^s + p(X-1)^r \sum_{i=0}^{s-r-1} b_i(X-1)^i \right\rangle$ is principal. Then we have

$$\begin{aligned}
\mathcal{I} &= \left\langle (X-1)^s + p(X-1)^t \sum_{i=0}^{T-t-1} a_i(X-1)^i, p(X-1)^T \right\rangle \\
&= \left\langle (X-1)^s + p(X-1)^r \sum_{i=0}^{s-r-1} b_i(X-1)^i \right\rangle \\
&= \left\langle (X-1)^s + p(X-1)^r \sum_{i=0}^{T-r-1} b_i(X-1)^i, p(X-1)^T \right\rangle,
\end{aligned}$$

where the third equality comes from the fact that $p(X-1)^T \in \mathcal{I}$. Now by the uniqueness we must have $r = t$ and $a_i = b_i$ for all $0 \le i \le T-t-1$. Therefore

$$\mathcal{I} = \left\langle (X-1)^s + p(X-1)^t \sum_{i=0}^{T-t-1} a_i(X-1)^i + p(X-1)^T \sum_{i=0}^{T-t-1} b_{i+T}(X-1)^i \right\rangle.$$

Now, by an easy verification, one can conclude that

$$p(X-1)^T \in \left\langle (X-1)^s + p(X-1)^t \sum_{i=0}^{T-t-1} a_i(X-1)^i \right\rangle,$$

which is a contradiction. Hence these ideals are non-principal. □

Let us, for convenience, denote $p-1$ and $p-2$ by α and β, respectively. The proof process of the following theorem is the same as that for Theorem 2.6 in [11].

Theorem 4.3. *The number of distinct ideals of $\mathcal{R}$ are as follows:*

(1) *The number of distinct principal ideals of $\mathcal{R}$ is equal to*

$$4\left(\frac{p^{mp^{n-1}}-1}{p^m-1}\right) + (2\beta p^{n-1}+1)p^{mp^{n-1}}.$$

(2) *The number of distinct non-principal ideals of $\mathcal{R}$ is equal to*

$$(p^m+3)\left(\frac{p^{mp^{n-1}}-1}{(p^m-1)^2} - \frac{p^{n-1}}{p^m-1}\right) + 2\beta p^{n-1}\left(\frac{p^{mp^{n-1}}-1}{p^m-1}\right) + p^{n-1}.$$

(3) *The total number of distinct ideals of $\mathcal{R}$, denoted $\mathcal{N}_m$, is:*

$$\begin{aligned}
\mathcal{N}_m = {} & (2p+1) + (2\beta p^{n-1}+1)p^{mp^{n-1}} + (5p^m-1)p^m\left(\frac{p^{mp^{n-1}-1}-1}{(p^m-1)^2}\right) \\
& - 4\frac{p^{n-1}-1}{p^m-1} + 2\beta\left(p^{n-1}\left(\frac{p^{mp^{n-1}}-1}{p^m-1}\right) - 1\right).
\end{aligned}$$

Proof. The proof is omitted as it is similar to that for Theorem 2.6 of [11]. Note that when $p = 2$, this theorem matches with Theorem 2.6 of [11]. □

In the rest of the section we assume that $p \neq 2$ and describe self-dual ideals in the ring $\mathcal{R}$.

Corollary 4.4. *The following table lists all distinct ideals of the ring $\mathscr{R}$ together with their annihilators.*

Case	$\mathscr{I}$ *and* $A(\mathscr{I})$
1.	$\mathscr{I} = \langle 0\rangle, \quad A(\mathscr{I}) = \langle 1\rangle$
2.	$\mathscr{I} = \langle 1\rangle, \quad A(\mathscr{I}) = \langle 0\rangle$
3.	$\mathscr{I} = \langle p\rangle, \quad A(\mathscr{I}) = \langle p\rangle$
4.	$\mathscr{I} = \langle p(X-1)^s\rangle, \ (1 \le s \le p^n - 1), \quad A(\mathscr{I}) = \langle p, (X-1)^{p^n-s}\rangle$
5.	$\mathscr{I} = \langle (X-1)^s\rangle, \ (1 \le s \le p^{n-1}), \quad A(\mathscr{I}) = \left\langle (X-1)^{p^n-s} + p(X-1)^{p^{n-1}-s}\left(-\mathscr{K}(X)\right)\right\rangle$
6.	$\mathscr{I} = \langle (X-1)^s\rangle, \ (p^{n-1}+1 \le s \le p^n - 1)$ $A(\mathscr{I}) = \left\langle (X-1)^{\alpha p^{n-1}} + p\left(-\mathscr{K}(X)\right), p(X-1)^{p^n-s}\right\rangle$
7.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^{s-\alpha p^{n-1}}\left(-\mathscr{K}(X)\right)\right\rangle, \quad (\alpha p^{n-1} \le s \le p^n - 1)$ $A(\mathscr{I}) = \left\langle (X-1)^{p^n-s}\right\rangle$
8.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^{s-\alpha p^{n-1}}\left(-\mathscr{K}(X) + (X-1)^v\widetilde{h}(X)\right)\right\rangle$ $(\alpha p^{n-1} \le s \le p^{n-1} + v, \ v \ge 1)$ $A(\mathscr{I}) = \left\langle (X-1)^{p^n-s} + p(X-1)^{p^{n-1}+v-s}\left(-\widetilde{h}(X)\right)\right\rangle$
9.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^{s-\alpha p^{n-1}}\left(-\mathscr{K}(X) + (X-1)^v\widetilde{h}(X)\right)\right\rangle$ $(p^{n-1} + v < s \le p^n - 1, \ s > \alpha p^{n-1}, \ v \ge 1)$ $A(\mathscr{I}) = \left\langle (X-1)^{\alpha p^{n-1}-v} + p\left(-\widetilde{h}(X)\right), p(X-1)^{p^n-s}\right\rangle$
10.	$\mathscr{I} = \left\langle (X-1)^{\alpha p^{n-1}} + p\left(-\mathscr{K}(X) + (X-1)^v\widetilde{h}(X)\right)\right\rangle, \quad (p^{n-1} + v < \alpha p^{n-1}, \ v \ge 1)$ $A(\mathscr{I}) = \left\langle (X-1)^{\alpha p^{n-1}-v} + p\left(-\widetilde{h}(X)\right)\right\rangle$
11.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^{s-\alpha p^{n-1}}h(X)\right\rangle, \quad (\alpha p^{n-1} < s \le p^n - 1, \ h_0 \ne 0, 1)$ $A(\mathscr{I}) = \left\langle (X-1)^{\alpha p^{n-1}} + p\left(1 - h(X)\right), p(X-1)^{p^n-s}\right\rangle$
12.	$\mathscr{I} = \left\langle (X-1)^{\alpha p^{n-1}} + ph(X)\right\rangle, \ (h_0 \ne 0, 1), \quad A(\mathscr{I}) = \left\langle (X-1)^{\alpha p^{n-1}} + p\left(1 - h(X)\right)\right\rangle$
13.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^t h(X)\right\rangle, \quad (p^n + t - s \ne p^{n-1}, \ s \le p^{n-1}, \ h(X) \ne 0)$ $A(\mathscr{I}) = \left\langle (X-1)^{p^n-s} + p(X-1)^{p^{n-1}-s}\left(-\mathscr{K}(X) + (X-1)^{\alpha p^{n-1}+t-s}\left(-h(X)\right)\right)\right\rangle$
14.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^t h(X)\right\rangle$ $(p^n + t - s \ne p^{n-1}, \ p^{n-1} < s < \alpha p^{n-1} + t, \ t > 0, \ h(X) \ne 0)$ $A(\mathscr{I}) = \left\langle (X-1)^{\alpha p^{n-1}} + p\left(-\mathscr{K}(X) + (X-1)^{\alpha p^{n-1}+t-s}\left(-h(X)\right)\right), p(X-1)^{p^n-s}\right\rangle$
15.	$\mathscr{I} = \langle (X-1)^s + ph(X)\rangle, \quad (p^{n-1} < s < \alpha p^{n-1}, \ h(X) \ne 0)$ $A(\mathscr{I}) = \left\langle (X-1)^{\alpha p^{n-1}} + p\left(-\mathscr{K}(X) + (X-1)^{\alpha p^{n-1}-s}\left(-h(X)\right)\right)\right\rangle$
16.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^t h(X)\right\rangle$ $(p^n + t - s \ne p^{n-1}, \ s > \alpha p^{n-1} + t, \ h(X) \ne 0, \ t > 0)$ $A(\mathscr{I}) = \left\langle (X-1)^{s-t} + p\left(-h(X) + (X-1)^{s-t-\alpha p^{n-1}}\right), p(X-1)^{p^n-s}\right\rangle$
17.	$\mathscr{I} = \langle (X-1)^s + ph(X)\rangle, \quad (s > \alpha p^{n-1}, \ h(X) \ne 0)$ $A(\mathscr{I}) = \left\langle (X-1)^s + p\left(-h(X) + (X-1)^{s-\alpha p^{n-1}}\right)\right\rangle$
18.	$\mathscr{I} = \left\langle (X-1)^s, p(X-1)^l\right\rangle, \quad (1 \le s \le p^n - 1, \ 0 \le l \le \min\{s, p^{n-1}\})$ $A(\mathscr{I}) = \left\langle (X-1)^{p^n-1} + p(X-1)^{p^{n-1}-l}\left(-\mathscr{K}(X)\right), p(X-1)^{p^n-s}\right\rangle$
19.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^{s-\alpha p^{n-1}}\left(-\mathscr{K}(X)\right), p(X-1)^l\right\rangle$ $(\alpha p^{n-1} \le s \le p^n - 1, s - \alpha p^{n-1} < l < s)$ $A(\mathscr{I}) = \left\langle (X-1)^{p^n-l}, p(X-1)^{p^n-s}\right\rangle$
20.	$\mathscr{I} = \left\langle (X-1)^s + p(X-1)^{s-\alpha p^{n-1}}\left(-\mathscr{K}(X) + (X-1)^v\widetilde{h}(X)\right), p(X-1)^l\right\rangle$ $(\alpha p^{n-1} < s \le p^n - 1, \ v \ge 1, \ s - \alpha p^{n-1} < l < \min\{s, p^{n-1} + v\})$ $A(\mathscr{I}) = \left\langle (X-1)^{p^n-l} + p(X-1)^{p^{n-1}+v-l}\left(-\widetilde{h}(X)\right), p(X-1)^{p^n-s}\right\rangle$

Case	$\mathcal{I}$ and $A(\mathcal{I})$
21.	$\mathcal{I}=\left\langle (X-1)^{\alpha p^{n-1}}+p\left(-\mathscr{K}(X)+(X-1)^{v}\widetilde{h}(X)\right),p(X-1)^{l}\right\rangle$
	$(0<l<\min\{\alpha p^{n-1},p^{n-1}+v\},\ v\geq 1)$
	$A(\mathcal{I})=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^{n-1}+v-l}\left(-\widetilde{h}(X)\right)\right\rangle$
22.	$\mathcal{I}=\left\langle (X-1)^{s}+p(X-1)^{s-\alpha p^{n-1}}h(X),p(X-1)^{l}\right\rangle$
	$(\alpha p^{n-1}<s\leq p^n-1,\ h_0\neq 0,1,\ s-\alpha p^{n-1}<l<p^{n-1})$
	$A(\mathcal{I})=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^{n-1}-l}\left(1-h(X)\right),p(X-1)^{p^n-s}\right\rangle$
23.	$\mathcal{I}=\left\langle (X-1)^{\alpha p^{n-1}}+ph(X),p(X-1)^{l}\right\rangle,\ (h_0\neq 0,1,\ 0<l<p^{n-1})$
	$A(\mathcal{I})=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^{n-1}-l}\left(1-h(X)\right)\right\rangle$
24.	$\mathcal{I}=\left\langle (X-1)^{s}+p(X-1)^{t}h(X),p(X-1)^{l}\right\rangle$
	$(p^n+t-s\neq p^{n-1},\ h(X)\neq 0,\ 1\leq s<\alpha p^{n-1}+t,\ 0<t<l<\min\{s,p^{n-1}\})$
	$A(\mathcal{I})=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^{n-1}-l}\left(-\mathscr{K}(X)+(X-1)^{\alpha p^{n-1}+t-s}\left(-h(X)\right)\right),p(X-1)^{p^n-s}\right\rangle$
25.	$\mathcal{I}=\left\langle (X-1)^{s}+ph(X),p(X-1)^{l}\right\rangle$
	$(1\leq s<\alpha p^{n-1},\ h(X)\neq 0,\ 0<l<\min\{s,p^{n-1}\})$
	$A(\mathcal{I})=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^{n-1}-l}\left(-\mathscr{K}(X)+(X-1)^{\alpha p^{n-1}+t-s}\left(-h(X)\right)\right)\right\rangle$
26.	$\mathcal{I}=\left\langle (X-1)^{s}+p(X-1)^{t}h(X),p(X-1)^{l}\right\rangle$
	$(p^n+t-s\neq p^{n-1},\ h(X)\neq 0,\ t>0,\ s>\alpha p^{n-1}+t,\ 0<t<l<p^n+t-s)$
	$A(\mathcal{I})=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^n+t-s-l}\left(-h(X)+(X-1)^{s-t-\alpha p^{n-1}}\right),p(X-1)^{p^n-s}\right\rangle$
27.	$\mathcal{I}=\left\langle (X-1)^{s}+ph(X),p(X-1)^{l}\right\rangle,\quad (s>\alpha p^{n-1},\ h(X)\neq 0,\ 0<l<p^n-s)$
	$A(\mathcal{I})=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^n+t-s-l}\left(-h(X)+(X-1)^{s-\alpha p^{n-1}}\right)\right\rangle$

Proof. This follows from Theorems 4.1 and 3.4. ■

Though the remaining results of this section are proved as their counterparts given in [11] for $p=2$, for self-sufficiency, we prefer to provide them with their proofs.

Lemma 4.5. *Suppose that $\mathcal{I}$ is an ideal of $\mathscr{R}$. If $\mathcal{I}=A(\mathcal{I})^*$ then $\mathcal{I}$ belongs to one of the following 6 cases from among the 27 cases given above.*

- $\langle p\rangle$ *(case 3).*
- $\left\langle (X-1)^{\alpha p^{n-1}}+ph(X)\right\rangle,\ (h_0\neq 0,1)$ *(case 12).*
- $\langle (X-1)^{s}+ph(X)\rangle,\ (s>\alpha p^{n-1},\ h(X)\neq 0)$ *(case 17).*
- $\left\langle (X-1)^{s},p(X-1)^{p^n-s}\right\rangle,\ (2s\geq \alpha p^{n-1}+p^n)$ *(case 18).*
- $\left\langle (X-1)^{s}+p(X-1)^{s-\alpha p^{n-1}}h(X),p(X-1)^{p^n-s}\right\rangle,\ (2s\geq \alpha p^{n-1}+p^n)$ *(case 22).*
- $\left\langle (X-1)^{s}+p(X-1)^{t}h(X),p(X-1)^{p^n-s}\right\rangle,\ (0<t<p^n-s,\ s>\alpha p^{n-1}+t)$ *(case 26).*

Proof. Note that for an ideal $\mathcal{I}$ of $\mathscr{R}$ we have $\mathrm{Tor}(A(\mathcal{I}))=\mathrm{Tor}(A(\mathcal{I})^*)$ and $\mathrm{Res}(A(\mathcal{I}))=\mathrm{Res}(A(\mathcal{I})^*)$. Clearly, cases 1 and 2 cannot be included. In cases 4, 6, 9, 11, 14, 16, 21, 23, 25 and 27, the ideals $\mathcal{I}$ and $A(\mathcal{I})$ are not of the same type in the sense that one of them is principal and the other one is non-principal, and hence the ideals included in these cases do not satisfy condition $\mathcal{I}=A(\mathcal{I})^*$. For cases 5, 7, 8, 10, 13 and 15 we have either $\mathrm{Tor}(\mathcal{I})\neq\mathrm{Tor}(A(\mathcal{I})^*)$ or $\mathrm{Res}(\mathcal{I})\neq\mathrm{Res}(A(\mathcal{I})^*)$, and hence these cases also fail to satisfy the mentioned condition. Cases 19, 20 and 24 do not satisfy the condition either; due to the similarity of the arguments, we just consider case 20. In this case, if $\mathcal{I}=A(\mathcal{I})^*$, then we must have

$$\begin{aligned}&\left\langle (X-1)^{s}+p(X-1)^{s-\alpha p^{n-1}}\left(-\mathscr{K}(X)+(X-1)^{v}\widetilde{h}(X)\right),p(X-1)^{l}\right\rangle\\&\quad=\left\langle (X-1)^{p^n-l}+p(X-1)^{p^{n-1}+v-l}G(X),p(X-1)^{p^n-s}\right\rangle,\end{aligned}$$

for some polynomial $G(X)$. Thus $p^n-s=l$ and hence

$$(X-1)^{s-\alpha p^{n-1}}\left(-\mathscr{K}(X)+(X-1)^{v}\widetilde{h}(X)-(X-1)^{v}G(X)\right)\in\mathrm{Tor}_1(\mathcal{I})=\left\langle (X-1)^{l}\right\rangle.$$

It follows from $v\geq 1$ that $s-\alpha p^{n-1}\geq l$ which is against condition $l>s-\alpha p^{n-1}$ in case 20. Therefore, only cases 3,12,17,18,22 and 26 are left, and it is easy to verify that ideals lying in these cases may satisfy $\mathcal{I}=A(\mathcal{I})^*$ provided that they have the extra conditions mentioned in the Lemma. ■

Corollary 4.6. *There are only two cyclic self-dual codes of length p over* $\mathrm{GR}(p^2, m)$, *namely* $\mathcal{I}_1 = \langle p\rangle$ *and* $\mathcal{I}_2 = \left\langle (X-1)^{\alpha} + p(2^{-1})\right\rangle$.

Proof. Clearly $\langle p\rangle$ is a self-dual code. Suppose that $\mathcal{I} = \langle (X-1)^{\alpha} + pa\rangle$, $a \in \tau_m$, is an ideal of the form given in case 12. Condition $\mathcal{I} = A(\mathcal{I})^*$ implies that $\langle (X-1)^{\alpha} + pa\rangle = \langle (X-1)^{\alpha} + p(1-a)X^{\alpha}\rangle$, which is true iff $a = 2^{-1}$. Obviously, other cases in Lemma 4.5 give no ideal. ■

We should mention that in the case $p = 2$ there is only one cyclic self-dual code of length 2 over $\mathrm{GR}(4, m)$, namely the code $\langle 2\rangle$ (part (i) of [11, Corollary 5.6]).

Corollary 4.7. *Suppose that C is a cyclic code of length 9 over* $\mathrm{GR}(9, m)$. *Then C is self-dual iff it is one of the following codes:*

$$\begin{cases} \langle 3\rangle, \left\langle (X-1)^6 + 3\left(2 + a(X-1) + a(X-1)^2\right)\right\rangle, \\ \left\langle (X-1)^7 + 3\left(c + 2(1+c)(X-1)\right)\right\rangle, \left\langle (X-1)^8, 3(X-1)\right\rangle \end{cases}$$

where $a \in \tau_m$. *Therefore, the number of cyclic self-dual codes of length 9 over* $\mathrm{GR}(9, m)$ *is* $2 + 2 * 3^m$.

Proof. Clearly $\langle 3\rangle$ is a self-dual code. Suppose

$$\mathcal{I} = \left\langle (X-1)^6 + 3\left(a_1 + a_2(X-1) + a_3(X-1)^2\right)\right\rangle \quad (a_1 \neq 0, 1)$$

is an ideal of the form given in case 12. Condition $\mathcal{I} = A(\mathcal{I})^*$ requires that

$$\begin{aligned} &\left\langle (X-1)^6 + 3\left(a_1 + a_2(X-1) + a_3(X-1)^2\right)\right\rangle \\ &\quad = \left\langle (X-1)^6 + 3\left((1-a_1)X^6 + a_2(X-1)X^5 - a_3(X-1)^2X^4\right)\right\rangle. \end{aligned}$$

This equality holds iff

$$a_1 - (1-a_1)X^6 + a_2(X-1)\left(1-X^5\right) + a_3(X-1)^2\left(1+X^4\right) \in \mathrm{Tor}_1(\mathcal{I}) = \left\langle (X-1)^3\right\rangle,$$

which holds iff $a_1 = 2$ and $a_2 = a_3$. The same argument applies to the other cases. ■

5. Negacyclic codes

Let $\mathscr{R}^-$ denote the ring $\mathrm{GR}(p^2, m)[X]/\left\langle X^N + 1\right\rangle$. Replacing $X^N - 1$ with $X^N + 1$, Theorem 2.1 provides a unique set of generators for ideals of the ring $\mathscr{R}^-$. Since the structure of negacyclic codes of length N, $(N, p) = 1$, over $\mathrm{GR}(p^2, m)$ has been studied in [10], we assume in this section that $p \mid N$.

Lemma 5.1. *If $p > 2$ then in $\mathscr{R}^-$ we have* $(X^k + 1)^{p^n} = p(X^k + 1)^{p^{n-1}}\mathscr{K}^-(X)$, *where*

$$\mathscr{K}^-(X) = \sum_{j=0}^{p-2} \frac{-1}{j+1}(X^k + 1)^{jp^{n-1}} \in \mathbb{F}_{p^m}[X].$$

In particular, $\mathscr{K}^-(X)$ is a unit in $\mathscr{R}^-$.

Proof. The proof is omitted as it is similar to that for Lemma 2.2. ■

Suppose that $p > 2$. It is deduced from this Lemma that Theorem 2.3 is still valid for $\mathscr{R}^-$ by replacing $X^N - 1$ with $X^N + 1$, $X^{N/p} - 1$ with $X^{N/p} + 1$ and $\mathscr{K}(X)$ with $\mathscr{K}^-(X)$. This shows that one can obtain the unique form of ideals of $\mathscr{R}^-$ in a way similar to the one applied on $\mathscr{R}$. Applying the same arguments used in Section 3, one can describe the dual of ideals of the ring $\mathscr{R}^-$ as well. Theorem 4.1 is still valid if we replace the term $(X-1)$ by $(X+1)$ and the polynomial $\mathscr{K}(X)$ by $\mathscr{K}^-(X)$. Consequently, when $N = p^n$ and $p > 2$, the number of distinct ideals of $\mathscr{R}^-$ is equal to the number of distinct ideals of $\mathscr{R}$, which is obtained by Theorem 4.3.

Now let $p = 2$. The following useful lemma is indeed Lemma 3.1 in [9].

Lemma 5.2. *Suppose that $p = 2$. Then in $\mathscr{R}^-$ we have* $(X^k + 1)^{2^n} = 2\mathscr{U}(X)$, *where $\mathscr{U}(X)$ is a unit.*

Proof. The result is obtained by replacing X with X^k in Lemma 3.1 of [9]. ■

Recall that $X^N + 1 = f_1(X)^{2^n} f_2(X)^{2^n} \ldots f_r(X)^{2^n}$ is the unique factorization of $X^N + 1$ over $\mathbb{F}_{2^m}$. The following theorem now provides a brief classification of ideals of $\mathscr{R}^-$ when $p = 2$, namely ideals of the ring $\mathrm{GR}(4, m)[X]/\left\langle X^N + 1\right\rangle$.

Theorem 5.3. *Let $p = 2$ and $\mathcal{I}$ be an ideal of $\mathscr{R}^-$. Then we have* $\mathcal{I} = \left\langle \prod_{i=1}^r f_i(X)^{a_i}\right\rangle$, *where* $0 \leq a_i \leq 2^{n+1}$ *and the polynomial* $\prod_{i=1}^r f_i(X)^{a_i}$ *is calculated in $\mathscr{R}^-$. Moreover,* $\mathrm{Res}(\mathcal{I}) = \left\langle \prod_{i=1}^r f_i(X)^{b_i}\right\rangle$ *and* $\mathrm{Tor}(\mathcal{I}) = \left\langle \prod_{i=1}^r f_i(X)^{c_i}\right\rangle$, *where* $b_i = \min\{a_i, 2^n\}$ *and* $c_i = \max\{a_i, 2^n\} - 2^n$.

Proof. Assume that $\mathrm{Res}(\mathcal{I}) = \langle f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r} \rangle$. Then $\mathcal{I}$ contains a polynomial $A(X)$ of the form $A(X) = f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r} + 2H(X)$, where the polynomial $f_1(X)^{j_1} f_2(X)^{j_2} \dots f_r(X)^{j_r}$ is calculated in $\mathscr{R}$. Let $S(X)$ be the polynomial $f_1(X)^{2^n - j_1} f_2(X)^{2^n - j_2} \dots f_r(X)^{2^n - j_r}$. Using Lemma 5.2 we have

$$S(X)A(X) = (X^k + 1)^{2^n} + 2H(X)S(X) = 2(\mathscr{U}(X) + H(X)S(X)).$$

This implies that $2(1 + \mathscr{U}^{-1}(X)H(X)S(X))$ lies in $\mathcal{I}$. Assume that $\mathrm{Tor}(\mathcal{I}) = \langle h(X) \rangle$, where $h(X) = f_1(X)^{l_1} f_2(X)^{l_2} \dots f_r(X)^{l_r}$. Then $h(X) \mid [1 + \mathscr{U}^{-1}(X)H(X)S(X)]$. Now if $j_i < 2^n$ then $f_i(X) \mid S(X)$ and hence $(f_i(X), 1 + \mathscr{U}^{-1}(X)H(X)S(X)) = 1$. This implies that $(f_i(X), h(X)) = 1$ or $l_i = 0$. Setting $G(X) := \prod_{i=1}^{r} f_i(X)^{j_i + l_i}$, we have $G(X) = A(X)h(X) - 2h(X)H(X) \in \mathcal{I}$ and hence $\langle G(X) \rangle \subseteq \mathcal{I}$. On the other hand, the relation between j_i and l_i guarantees that

$$\mathrm{Res}(\langle G(X) \rangle) = \mathrm{Res}\left(\left\langle \prod_{i=1}^{r} f_i(X)^{j_i + l_i} \right\rangle \right) = \left\langle \prod_{i=1}^{r} f_i(X)^{j_i} \right\rangle = \mathrm{Res}(\mathcal{I}).$$

Also using Lemma 5.2 we have $S(X)G(X) = (X^k + 1)^{2^n} h(X) = 2\mathscr{U}(X)h(X)$. This implies that $2h(X) \in \langle G(X) \rangle$ and hence $\mathrm{Tor}(\mathcal{I}) \subseteq \mathrm{Tor}(\langle G(X) \rangle)$. Consequently,

$$|\mathcal{I}| = |\mathrm{Res}(\mathcal{I})||\mathrm{Tor}(\mathcal{I})| \leq |\mathrm{Res}(\langle G(X) \rangle)||\mathrm{Tor}(\langle G(X) \rangle)| = |\langle G(X) \rangle|,$$

and hence $\mathcal{I} = \langle G(X) \rangle$. Setting $a_i := j_i + l_i$ completes the proof. ■

Remark 5.4. Theorem 5.3 specially classifies negacyclic codes of even length over $\mathbb{Z}_4$, which has been done in Theorem 2 of [4]. However, our classification is based on factorization of $X^k - 1$ over $\mathbb{F}_2$ while the classification presented in Theorem 2 of [4] is based on factorization of $X^k - 1$ over $\mathbb{Z}_4$. □

Theorem 5.5. *Let $p = 2$ and $\mathcal{I} = \left\langle \prod_{i=1}^{r} f_i(X)^{a_i} \right\rangle$ be an ideal of $\mathscr{R}^-$. Then we have $\mathcal{I}^\perp = \left\langle \prod_{i=1}^{r} f_i^*(X)^{2^{n+1} - a_i} \right\rangle$, where $f_i^*(X)$ denotes the reciprocal of $f_i(X)$.*

Proof. The proof follows from Theorem 5.3 and the fact that for an ideal $\mathcal{I}$ of $\mathscr{R}^-$ with $\mathrm{Res}(\mathcal{I}) = \langle f(X) \rangle$ and $\mathrm{Tor}(\mathcal{I}) = \langle h(X) \rangle$, we have $\mathrm{Res}(\mathcal{I}^\perp) = \left\langle \widehat{h(X)}^* \right\rangle$ and $\mathrm{Tor}(\mathcal{I}^\perp) = \left\langle \widehat{f(X)}^* \right\rangle$, where $\widehat{f(X)}$ stands for $(X^N + 1)/f(X)$. ■

Corollary 5.6. *Non-trivial self-dual negacyclic codes of even length over* $\mathrm{GR}(4, m)$ *exist if and only if there exists $f_i(X)$ for which $f_i^*(X) = \alpha(X) f_j(X)$, where $i \neq j$ and $\alpha(X)$ is a unit in $\mathscr{R}^-$.*

Proof. Assume that $\mathcal{I}$ satisfies $\mathcal{I} = \mathcal{I}^\perp$. If for all $1 \leq i \leq r$ we have $f_i(X) = \alpha_i(X) f_i^*(X)$, where $\alpha_i(X) \in \mathscr{R}^-$ are units, then according to Theorem 5.5 we must have $\mathcal{I} = \left\langle \prod_{i=1}^{r} f_i(X)^{2^n} \right\rangle = \langle 2 \rangle$, which is the trivial self-dual code. Conversely, assume that $f_i^*(X) = \alpha(X) f_j(X)$ for unit $\alpha(X) \in \mathscr{R}^-$ and $i \neq j$. Then the ideal generated by the polynomial

$$f_1(X)^{2^n} \dots f_{i-1}(X)^{2^n} f_i(X)^{2^{n+1}} f_{i+1}(X)^{2^n} \dots f_{j-1}(X)^{2^n} f_j(X)^0 f_{j+1}(X)^{2^n} \dots f_r(X)^{2^n}$$

is a non-trivial self-dual negacyclic code. ■

6. Summary

A unique set of generators for cyclic codes of arbitrary length over the Galois ring $\mathrm{GR}(p^2, m)$ was introduced and an algorithm producing these generators was given. The form of dual codes of these codes was studied. More precise results for cyclic codes of length p^n over the ring $\mathrm{GR}(p^2, m)$ were given. The obtained results on cyclic codes were extended to the class of negacyclic codes.

Acknowledgment

The authors would like to thank an anonymous referee whose comments greatly improved the manuscript.
This work was in part supported by a grant from Iran Telecommunication Research Center (ITRC).

Appendix

Definition A.1. Let $\mathbb{F}$ be a field and $f(X) = a_0 + a_1 X + \dots + a_l X^l \in \mathbb{F}[X]$ be a polynomial. The first order derivative of $f(X)$ is the polynomial $f'(X) = a_1 + 2a_2 X + \dots + l a_l X^{l-1}$. The higher order derivatives of $f(X)$ are defined in a similar way. We denote the lth order derivative of $f(X)$ by $f^{(l)}$.

It is easy to verify that if $f(X) = a_0 + a_1(X - 1) + \dots + a_l(X - 1)^l \in \mathbb{F}[X]$ then $i! a_i = f^{(i)}(1)$.

The Proof of Lemma 2.2. Let us denote $a \pmod{p^2}$ and $a \pmod{p}$ by $[a]_2$ and $[a]_1$, respectively. Suppose that $p \neq 2$. Since

$$(X-1)^p = X^p - 1 + \sum_{i=1}^{p-1} (-1)^i \left[\binom{p}{i}\right]_2 X^{p-i}$$

and

$$\begin{aligned}\left[\binom{p}{i}\right]_2 &= \left[\frac{p!}{i!(p-i)!}\right]_2 = \left[\frac{p(p-1)\dots(p-i+1)}{1\times 2\times\cdots\times i}\right]_2 \\ &= \left[\frac{(-1)^{i-1}(i-1)!p}{i!}\right]_2 = \left[\frac{(-1)^{i-1}p}{i}\right]_2 \\ &= p\left[\frac{(-1)^{i-1}}{i}\right]_1,\end{aligned}$$

we have

$$(X-1)^p = X^p - 1 + p\sum_{i=1}^{p-1}\left[-\frac{1}{i}\right]_1 X^{p-i}.$$

Set $g(X) := \sum_{i=1}^{p-1}\left[-\frac{1}{i}\right]_1 X^{p-i} \in \mathbb{F}_p[X]$. It is easy to verify that for $1 \le j \le p-1$ we have

$$g^{(j)}(1) = \sum_{i=1}^{p-j}(-1)^{j-1}\left[\frac{(i+j-1)!}{i!}\right]_1.$$

Since $g(1) = 0$, $g(X)$ is in the form $g(X) = a_1(X-1) + a_2(X-1)^2 + \cdots + a_{p-1}(X-1)^{p-1}$, where $(j!)a_j = g^{(j)}(1)$ and we have

$$\begin{aligned}a_j &= \left[\frac{1}{j!}\sum_{i=1}^{p-j}(-1)^{j-1}\frac{(i+j-1)!}{i!}\right]_1 = \left[\sum_{i=1}^{p-j}\frac{(-1)^{j-1}}{j}\binom{i+j-1}{i}\right]_1 \\ &= \left[\frac{(-1)^{j-1}}{j}\right]_1\left[\sum_{i=1}^{p-j}\binom{i+j-1}{i}\right]_1 = \left[\frac{(-1)^{j-1}}{j}\right]_1\left[\binom{p}{p-j}-1\right]_1 \\ &= \left[\frac{(-1)^j}{j}\right]_1.\end{aligned}$$

The fourth equality follows from the fact that $\sum_{i=1}^{l}\binom{n+i}{i} = \binom{n+l+1}{l} - 1$. Consequently,

$$(X-1)^p = X^p - 1 + p(X-1)\sum_{j=0}^{p-2}\left[\frac{(-1)^{j+1}}{j+1}\right]_1 (X-1)^j.$$

An induction process shows that

$$(X-1)^{p^n} = X^{p^n} - 1 + p(X-1)^{p^{n-1}}\sum_{j=0}^{p-2}\left[\frac{(-1)^{j+1}}{j+1}\right]_1 (X-1)^{jp^{n-1}}.$$

Replacing X by X^k gives us the result. For the case $p = 2$ we note that $(X-1)^2 = X^2 - 1 + 2(X-1)$ and hence $\mathscr{K}(X) = 1$ in this case.

References

[1] T. Abualrub, A. Ghrayeb, R. Oehmke, A mass formula and rank of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inform. Theory 50 (12) (2004) 3306–3312.
[2] T. Abualrub, R. Oehmke, On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e, IEEE Trans. Inform. Theory 49 (9) (2003) 2126–2133.
[3] T. Abualrub, R. Oehmke, Cyclic codes of length 2^e over $\mathbb{Z}_4$, Discrete Appl. Math. 128 (2003) 3–9.
[4] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, Discrete Appl. Math. 128 (2003) 27–46.
[5] T. Blackford, Negacyclic codes over $\mathbb{Z}_4$ of even length, IEEE Trans. Inform. Theory 49 (9) (2003) 1417–1424.
[6] E. Byrne, P. Fitzpatrick, Gröbner bases over Galois rings with an application to decoding alternate codes, J. Symbolic Comput. 31 (2001) 565–584.
[7] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Des. Codes Cryptogr. 6 (1995) 21–35.
[8] G. Castagnoli, J.M. Massey, P.A. Schoeller, N. Seemann, On repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 337–342.
[9] H.Q. Dinh, Negacyclic codes of length 2^s over Galois rings, IEEE Trans. Inform. Theory 51 (12) (2005) 4252–4262.
[10] H.Q. Dinh, S.R. Lopez-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory 50 (8) (2004) 1728–1744.
[11] S.T. Dougherty, S. Ling, Cyclic codes over $\mathbb{Z}_4$ of even length, Des. Codes Cryptogr. 39 (2) (2006) 127–153.

[12] S.T. Dougherty, Y.H. Park, On modular cyclic codes, Finite Fields Appl. 13 (2007) 31–57.
[13] A.R. Hammons, P.V. Kummar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[14] P. Kanwar, S.R. López-Permouth, Cyclic codes over the integers modulo p^m, Finite Fields Appl. 3 (1997) 334–352.
[15] A.A. Nechaev, D.A. Mikhailov, Canonical generating system of a monic polynomial ideal over a commutative artinian chain ring, Discrete Appl. Math. 11 (2001) 545–586.
[16] G.H. Norton, A. Salagean, Cyclic codes and minimal strong gröbner bases over a principal ideal ring, Finite Fields Appl. 9 (2003) 237–249.
[17] G.H. Norton, A. Salagean, On the structure of linear and cyclic codes over a finite chain ring, AAECC 10 (2000) 489–506.
[18] A. Salagean, Repeated-root cyclic and negacyclic codes over a finite chain ring, Discrete Appl. Math. 154 (2006) 413–419.
[19] J. Wolfman, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (1999) 2527–2532.